

Docket No.: 67161-089

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of	:	Customer Number: 20277
	:	
Shigenori MIYAUCHI, et al.	:	Confirmation Number:
	:	
Serial No.:	:	Group Art Unit:
	:	
Filed: August 26, 2003	:	Examiner: Unknown
	:	
For: ENCRYPTION CIRCUIT ACHIEVING HIGHER OPERATION SPEED	:	

**CLAIM OF PRIORITY AND  
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT**

Mail Stop CPD  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

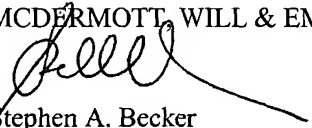
In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claims the priority of:

**Japanese Patent Application No. 2002-310009, filed October 24, 2002**

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

  
Stephen A. Becker  
Registration No. 26,527

600 13<sup>th</sup> Street, N.W.  
Washington, DC 20005-3096  
(202) 756-8000 SAB:tlb  
Facsimile: (202) 756-8087  
**Date: August 26, 2003**

67161-089  
MIYAUCHI et al.  
August 26, 2003

日 本 国 特 許 庁

JAPAN PATENT OFFICE

*McDermott, Will & Emery*

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月24日

出 願 番 号

Application Number:

特願2002-310009

[ ST.10/C ]:

[ JP 2002-310009 ]

出 願 人

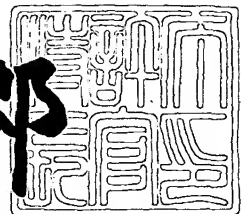
Applicant(s):

三菱電機株式会社

2002年11月26日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2002-3093483



【書類名】 特許願

【整理番号】 541973JP01

【提出日】 平成14年10月24日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00  
H04L 9/14

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会  
社内

【氏名】 宮内 成典

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会  
社内

【氏名】 山口 敦男

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100083703

【弁理士】

【氏名又は名称】 仲村 義平



【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【選任した代理人】

【識別番号】 100098316

【弁理士】

【氏名又は名称】 野田 久登

【選任した代理人】

【識別番号】 100109162

【弁理士】

【氏名又は名称】 酒井 將行

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号回路

【特許請求の範囲】

【請求項 1】 接続された複数の演算回路と、

前記複数の演算回路を制御して、暗号化または復号の制御を行なう制御回路とを含んだ暗号回路であって、

前記複数の演算回路はそれぞれ、演算データを保持する第 1 のレジスタと、

前記第 1 のレジスタに保持される演算データに対して加減算を実行する加減算回路と、

前記加減算回路による演算結果に対して右シフトを実行する右シフト回路と、

前記右シフト回路による演算結果を保持する第 2 のレジスタとを含み、

第 1 の演算回路の加減算回路は、第 2 の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第 3 の演算回路へ出力し、

前記第 1 の演算回路の右シフト回路は、前記第 3 の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を前記第 2 の演算回路へ出力する、暗号回路。

【請求項 2】 前記制御回路は、演算データを分割して前記複数の演算回路の第 1 のレジスタに格納する、請求項 1 記載の暗号回路。

【請求項 3】 前記第 1 の演算回路の加減算回路は、第 1 のクロックで演算データを確定し、

前記第 3 の演算回路の加減算回路は、前記第 1 のクロックよりも 1 クロック遅れた第 2 のクロックで演算データおよび前記第 1 の演算回路からのキャリーアウトを確定する、請求項 1 または 2 記載の暗号回路。

【請求項 4】 前記第 1 の演算回路の加減算回路は、第 1 のクロックで演算データを確定し、

前記第 1 の演算回路の第 2 のレジスタは、前記第 1 のクロックよりも 1 クロック遅れた第 2 のクロックで最上位ビット以外のビットが書込まれ、前記第 2 のクロックよりも半クロック遅れた第 3 のクロックで最上位ビットが書込まれる、請

求項 1 または 2 記載の暗号回路。

【請求項 5】 前記複数の演算回路は、キャリーアウト信号およびシフトアウト信号がループするように接続される、請求項 1～4 のいずれかに記載の暗号回路。

【請求項 6】 前記複数の演算回路のそれぞれは、さらに前記第 2 のレジスタに保持される演算結果に対して左シフトを実行する左シフト回路を含み、

前記第 1 の演算回路の左シフト回路は、前記第 2 の演算回路からのシフトイン信号を用いて左シフトを実行し、左シフトによって発生するシフトアウト信号を前記第 3 の演算回路へ出力する、請求項 1～5 のいずれかに記載の暗号回路。

【請求項 7】 前記第 1 の演算回路はさらに、前記第 3 の演算回路からのシフトイン信号と、前記第 1 の演算回路の左シフト回路からのシフトイン信号とを選択的に前記第 1 の演算回路の加減算回路へ出力するセレクタを含む、請求項 6 記載の暗号回路。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、使用される情報の暗号化技術および復号技術に関し、特に、べき乗剰余演算、モンゴメリ演算、加減算などの演算によってデータを暗号化および復号する暗号回路に関する。

【0 0 0 2】

【従来の技術】

情報通信技術の発展に伴い、情報ネットワーク上のセキュリティの確保（データの盗用や破壊を防止すること）が重要視されるようになってきている。そのため、情報の暗号化技術および復号技術が採用されることが多く、その適用分野は単なる情報通信分野に留まらず、交通、金融、医療、流通等の身近な分野にまで広がりつつある。この種の暗号化技術および復号技術には、高度なセキュリティを単純な原理によって実現できることが要求される。

【0 0 0 3】

これに関連する技術として、特開平 5 - 3 2 4 2 7 7 号公報および特開 2 0 0

2-229445号公報に開示された技術がある。

【0004】

特開平5-324277号公報に開示された暗号通信方法は、剰余演算  $Q = A \cdot B \bmod N$  およびべき乗剰余演算  $C = M^e \bmod N$  を、 $N$  と素な整数  $R$  を用いた同形の演算  $Z = U \cdot V \cdot R^{-1} \bmod N$  の繰返しにより実現するものである。

【0005】

また、特開2002-229445号公報に開示されたべき乗剰余演算回路は、鍵  $e$  を保持する  $e$  レジスタ、モンゴメリ変換をする乗算  $Y$  を保持する  $Y$  レジスタ、鍵  $N$  を保持する  $N$  レジスタ、モンゴメリ変換の演算時に行なう  $2B + N$  の値を保持する  $B2N$  レジスタ、平文  $X$  を保持する  $X$  レジスタ、暗号化および復号のための演算を行なう演算回路、演算結果  $P$  を保持する  $P$  レジスタなどを含み、高速処理を可能としたものである。

【0006】

【特許文献1】

特開平5-324277号公報

【0007】

【特許文献2】

特開2002-229445号公報

【0008】

【発明が解決しようとする課題】

現代の暗号は、秘密鍵を計算によって見つけることが時間的に困難であることを安全性の根拠としているものが多い。たとえば、RSA (Rivest-Shamir-Adleman scheme) 暗号を用いる場合、2つの素数の積である整数  $N$  ( $N = p \times q$ 、 $p$  および  $q$  は素数) を短時間で素因数分解することの難しさが安全性の根拠となっている。このことは、裏を返せば、今後コンピュータ等の計算機の性能が向上するに伴い、RSA暗号の安全性を確保するためには、選択する素数  $p$  および  $q$  の桁数を増やさなければならないことを意味している。

【0009】

ここで、上述した特開平5-324277号公報および特開2002-229

4 4 5 号公報に開示された発明によって、ビット長の長い暗号回路を構成した場合を考える。最も簡単な方法は、レジスタ群を増やして暗号回路を変更することである。しかし、レジスタ群が増加した分だけ演算時間が増加するとともに、レジスタの増加分だけ暗号回路が大きくなるため得策ではない。

#### 【 0 0 1 0 】

また、加減算回路が一度に扱えるビット長を、たとえば 1 2 8 ビットから 2 5 6 ビットに拡張した場合、加減算時におけるキャリーの伝播経路が長くなるため、動作周波数を上げることが困難になるといった問題点がある。

#### 【 0 0 1 1 】

本発明は、上記問題点を解決するためになされたものであり、その目的は、暗号回路の動作クロック周波数を高くでき、演算速度の高速化を図ることが可能な暗号回路を提供することである。

#### 【 0 0 1 2 】

##### 【課題を解決するための手段】

請求項 1 に記載の暗号回路は、接続された複数の演算回路と、複数の演算回路を制御して、暗号化または復号の制御を行なう制御回路とを含む。また、複数の演算回路はそれぞれ、演算データを保持する第 1 のレジスタと、第 1 のレジスタに保持される演算データに対して加減算を実行する加減算回路と、加減算回路による演算結果に対して右シフトを実行する右シフト回路と、右シフト回路による演算結果を保持する第 2 のレジスタとを含む。第 1 の演算回路の加減算回路は、第 2 の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第 3 の演算回路へ出力し、第 1 の演算回路の右シフト回路は、第 3 の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を第 2 の演算回路へ出力する。

#### 【 0 0 1 3 】

##### 【発明の実施の形態】

まず、本出願人が出願した特開 2 0 0 2 - 2 2 9 4 4 5 号公報、特願 2 0 0 1 - 1 6 3 7 1 9 号および特願 2 0 0 2 - 2 8 6 1 8 2 号に開示した暗号回路について簡単に説明する。



## 【 0 0 1 4 】

図 1 は、本出願人が出願した暗号回路の概略構成を示すブロック図である。この暗号回路 1 0 は、演算回路 1 2 と、演算回路 1 2 を制御して、べき乗剰余演算、モンゴメリ演算、加減算などの演算を実行する制御回路 1 1 とを含む。

## 【 0 0 1 5 】

図 2 は、演算回路 1 2 の概略構成を示すブロック図である。演算回路 1 2 は、鍵  $e$  を保持する 4 本の  $e$  レジスタ 1 2 1 と、モンゴメリ変換をする乗数  $Y$  を保持する 4 本の  $Y$  レジスタ 1 2 2 と、平文  $X$  を保持する 4 本の  $X$  レジスタ 1 2 3 と、鍵  $N$  を保持する 4 本の  $N$  レジスタ 1 2 4 と、モンゴメリ変換の演算時に行なう  $2B + N$  の値を保持する 4 本の  $B2N$  レジスタ 1 2 5 と、128 ビットの加減算回路 1 2 6 と、加減算回路 1 2 6 から出力される演算結果の最上位ビットの桁上り（キャリー）を保持する保持回路 1 2 7 と、128 ビットの右シフト回路 1 2 8 と、右シフト回路 1 2 8 によって右シフト処理が行なわれる際に発生する最下位ビットの桁落ち（シフトアウト）を他の右シフト処理時にシフトイン信号として使用するために保持する保持回路 1 2 9 と、右シフト回路 1 2 8 から出力される演算結果を一時的に保持する複数の  $P$  レジスタ 1 3 0 と、128 ビットの左シフト回路 1 3 1 と、左シフト回路 1 3 1 によって左シフト処理が行なわれる際に発生する最上位ビットの桁上り（シフトアウト）を他の左シフト処理時にシフトイン信号として使用するために保持する保持回路 1 3 2 とを含む。

## 【 0 0 1 6 】

べき乗剰余演算、モンゴメリ演算、RSA 暗号などの演算処理は、主として加算、減算、乗算および除算の繰返しによって実現されるため、制御回路 1 1 が図 2 に示す演算回路 1 2 を制御してそれぞれの演算アルゴリズムにしたがって演算を繰返し行なわせることによってこれらの演算処理が可能になる。なお、演算アルゴリズムの詳細は上述した文献を参照されたい。

## 【 0 0 1 7 】

## （第 1 の実施の形態）

図 3 は、本発明の第 1 の実施の形態における暗号回路の概略構成を示すブロック図である。この暗号回路 2 0 は、暗号回路 2 0 の全体的な制御を行なう制御回

路 2 1 と、4 つの演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) とを含む。本実施の形態においては、暗号方式として R S A 暗号を想定し、演算長として 5 1 2 ビットを想定しているが、これに限定されるものではない。

#### 【 0 0 1 8 】

制御回路 2 1 は、外部から受けた演算に必要となるデータをデータバスを介して演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) へ出力し、データバスを介して演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) から受けた演算結果を外部へ出力する。また、制御回路 2 1 は、R S A 暗号化または復号のアルゴリズムにしたがって演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) へ制御信号を出力し、演算処理を制御する。

#### 【 0 0 1 9 】

図 4 は、演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) の内部構成を説明するためのブロック図である。演算回路 0 ～ 3 ( 2 2 ～ 2 5 ) のそれぞれは、鍵 e を保持する e レジスタ 3 1 と、暗号化された平文 Y を保持する Y レジスタ 3 2 と、暗号化の対象となる平文 X を保持する X レジスタ 3 3 と、鍵 N を保持する N レジスタ 3 4 と、1 2 8 ビットの加減算回路 3 5 と、1 2 8 ビットの右シフト回路 3 6 と、右シフト回路 3 6 から出力される演算結果を一時的に保持する P レジスタ 3 7 と、1 2 8 ビットの左シフト回路 3 8 とを含む。

#### 【 0 0 2 0 】

加減算回路 3 5 は、e レジスタ 3 1、Y レジスタ 3 2、X レジスタ 3 3 または N レジスタ 3 4 に保持されるデータに対して加算または減算を行ない、演算結果を右シフト回路 3 6 へ出力する。また、加減算回路 3 5 は、演算結果の最上位ビットの桁上り ( キャリー ) を他の演算回路へキャリーアウト信号として出力し、他の演算回路からのキャリーアウト信号をキャリーイン信号として入力し、最下位ビットに設定する。

#### 【 0 0 2 1 】

右シフト回路 3 6 は、加減算回路 3 5 から出力された加減算結果を右シフトし、そのときに発生する最下位ビットの桁落ち ( シフトアウト ) を右シフトアウト信号として他の演算回路へ出力する。また、右シフト回路 3 6 は、他の演算回路からのシフトアウト信号をシフトイン信号として入力し、最上位ビットに設定す

る。

#### 【 0 0 2 2 】

左シフト回路 3 8 は、P レジスタ 3 7 に保持される値を左シフトし、そのときに発生する最上位ビットの桁上り（シフトアウト）を左シフトアウト信号として他の演算回路へ出力する。また、左シフト回路 3 8 は、他の演算回路からのシフトアウト信号をシフトイン信号として入力し、最下位ビットに設定する。

#### 【 0 0 2 3 】

制御回路 2 1 は、5 1 2 ビットの演算データを 1 2 8 ビットずつに分割し、演算回路 0 ～ 3 （ 2 2 ～ 2 5 ） のそれぞれの e レジスタ 3 1、Y レジスタ 3 2、X レジスタ 3 3 または N レジスタ 3 4 に格納する。たとえば、e レジスタに 5 1 2 ビットの演算データを格納する場合、演算回路 0 （ 2 2 ） 内の e レジスタ 3 1 に演算データのビット 0 ～ 1 2 7 を格納し、演算回路 1 （ 2 3 ） 内の e レジスタ 3 1 に演算データのビット 1 2 8 ～ 2 5 5 を格納し、演算回路 2 （ 2 4 ） 内の e レジスタ 3 1 に演算データのビット 2 5 6 ～ 3 8 3 を格納し、演算回路 3 （ 2 5 ） 内の e レジスタ 3 1 に演算データのビット 3 8 4 ～ 5 1 1 を格納する。

#### 【 0 0 2 4 】

演算回路 0 ～ 3 （ 2 2 ～ 2 5 ） におけるデータ演算は 1 クロック単位で実施され、演算回路 0 （ 2 2 ） から上位方向（演算回路 0 → 1 → 2 → 3 ） にキャリーが伝播される。右シフト回路 3 6 による右シフト処理はクロックによって遅らされることなく、上位の演算回路の動作クロックを利用して下位の演算回路にシフトインが行なわれる。この機能を実現するために、制御回路 2 1 は、P レジスタ 3 7 へのビット 0 ～ 1 2 6 のライト信号と、ビット 1 2 7 のライト信号とを独立制御している。

#### 【 0 0 2 5 】

図 5 は、演算回路における演算データの入力タイミングおよび P レジスタ 3 7 へのデータ書込みタイミングを説明するためのタイミングチャートである。クロック T 1 の立下りで演算回路 0 （ 2 2 ） への入力データが確定すると、加減算回路 3 5 からキャリーアウト信号が出力される。

#### 【 0 0 2 6 】

また、クロック T 2 の立下りで演算回路 0 ( 2 2 ) 内の P レジスタ 3 7 にデータのビット 0 ~ 1 2 6 が書込まれると共に、上位の演算回路 1 ( 2 3 ) への入力データが確定する。このタイミングでは、上位の演算回路 1 ( 2 3 ) の右シフトアウト信号が確定していないので、演算回路 0 ( 2 2 ) 内の P レジスタ 3 7 にデータのビット 1 2 7 を書込むことができない。したがって、クロック T 3 の立上りで演算回路 0 ( 2 2 ) 内の P レジスタ 3 7 にデータのビット 1 2 7 が書込まれる。なお、他の下位の演算回路と上位の演算回路との間の信号のタイミングは、この演算回路 0 ( 2 2 ) と演算回路 1 ( 2 3 ) との間の信号のタイミングと同様である。

#### 【 0 0 2 7 】

図 6 は、演算回路における演算データの入力および P レジスタ 3 7 へのデータ書込みが連続的に行なわれる場合のタイミングを説明するためのタイミングチャートである。図 5 に示すタイミングチャートとほぼ同様であるが、各クロックサイクルで 1 2 8 ビットの演算データが処理されることを示している。すなわち、演算回路 0 ~ 3 ( 2 2 ~ 2 5 ) は、5 1 2 ビットの演算データの処理を行なうのに 4 クロック必要である。しかし、乗算やモンゴメリ乗算剰余演算の繰返し演算など、加減算の結果の正負が次の演算種別に反映されない場合には、演算の完了を待たずに次の加減算を行なうことができるので、パイプライン的に処理を行なうことができ、実効的にはその 1 / 4 のクロック数 ( 1 クロック ) で演算を行なうことができる。

#### 【 0 0 2 8 】

以上説明したように、本実施の形態における暗号回路によれば、演算データを複数に分割し、複数の演算回路にそれぞれの演算データを演算させ、キャリーアウトおよびシフトアウトのみを上位の演算回路または下位の演算回路に出力するようにしたので、演算回路の回路規模を縮小することができると共に、キャリーの伝播経路を短くでき、動作クロック周波数を高くすることが可能となった。

#### 【 0 0 2 9 】

また、1 2 8 ビットの演算データを処理する演算回路と比較すると、同じクロック数で 4 倍の演算データを処理することができ、演算速度の高速化を図ること

が可能となった。

#### 【0030】

(第2の実施の形態)

図7は、本発明の第2の実施の形態における暗号回路の概略構成を示すブロック図である。本実施の形態における暗号回路は、図3に示す第1の実施の形態における暗号回路と比較して、演算回路3から出力されるキャリーアウト信号および左シフトアウト信号が演算回路0に入力され、演算回路0から出力される右シフトアウト信号が演算回路3に入力され、演算回路間をキャリーアウト信号およびシフトアウト信号がループしている点が異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。なお、本実施の形態においては、暗号方式としてRSA暗号を想定し、演算長として1024ビットを想定してるが、これに限定されるものではない。

#### 【0031】

図8は、本発明の第2の実施の形態における演算回路0～3(41～44)の内部構成を説明するためのブロック図である。本実施の形態における演算回路0～3(41～44)は、図4に示す第1の実施の形態における演算回路0～3(22～25)と比較して、eレジスタ、Yレジスタ、Xレジスタ、NレジスタおよびPレジスタが2本ずつ設けられている点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

#### 【0032】

制御回路21は、1024ビットの演算データを128ビットずつに分割し、演算回路0～3(41～44)のそれぞれのe0レジスタ51、Y0レジスタ52、X0レジスタ53、N0レジスタ54、e1レジスタ61、Y1レジスタ62、X1レジスタ63またはN1レジスタ64に格納する。

#### 【0033】

たとえば、eレジスタに1024ビットの演算データを格納する場合、制御回路21は、演算回路0(41)内のe0レジスタ51に演算データのビット0～127を格納し、演算回路1(42)内のe0レジスタ51に演算データのビット128～255を格納し、演算回路2(43)内のe0レジスタ51に演算デ

ータのビット 2 5 6 ~ 3 8 3 を格納し、演算回路 3 ( 4 4 ) 内の e 0 レジスタ 5 1 に演算データのビット 3 8 4 ~ 5 1 1 を格納する。

#### 【 0 0 3 4 】

また、制御回路 2 1 は、演算回路 0 ( 4 1 ) 内の e 1 レジスタ 6 1 に演算データのビット 5 1 2 ~ 6 3 9 を格納し、演算回路 1 ( 4 2 ) 内の e 1 レジスタ 6 1 に演算データのビット 6 4 0 ~ 7 6 7 を格納し、演算回路 2 ( 4 3 ) 内の e 1 レジスタ 6 1 に演算データのビット 7 6 8 ~ 8 9 5 を格納し、演算回路 3 ( 4 4 ) 内の e 1 レジスタ 6 1 に演算データのビット 8 9 6 ~ 1 0 2 3 を格納する。

#### 【 0 0 3 5 】

また、演算処理実行時には、1 2 8 ビット長のレジスタ群から適宜演算データを加減算回路 3 5 に設定することによって、各演算回路が見かけ上 2 5 6 ビット長の演算データを処理できるようになり、全体として 1 0 2 4 ビット長の演算データを処理することができるようになる。また、5 1 2 ビット長の演算データを処理する場合には、たとえば e 0 レジスタ 5 1、Y 0 レジスタ 5 2、X 0 レジスタ 5 3、N 0 レジスタ 5 4 および P 0 レジスタ 7 1 のみを使用することによって、5 1 2 ビット長の演算データの処理も行なうことができる。

#### 【 0 0 3 6 】

以上説明したように、本実施の形態における暗号回路によれば、レジスタ群をそれぞれ 2 本ずつ設け、演算回路間でキャリーアウト信号およびシフトアウト信号をループさせるようにしたので、第 1 の実施の形態において説明した効果に加えて、さらに演算データのビット長を容易に増やすことが可能となった。

#### 【 0 0 3 7 】

##### ( 第 3 の実施の形態 )

本発明の第 3 の実施の形態における暗号回路は、図 7 に示す第 2 の実施の形態における暗号回路と比較して、演算回路 0 ~ 3 の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

#### 【 0 0 3 8 】

図 9 は、第 3 の実施の形態における演算回路の内部構成を説明するためのブロック図である。図 8 に示す第 2 の実施の形態における演算回路の内部構成と比較

して、演算中に繰返し使用される固定データを、演算回路による演算の前に予め計算して格納するための B 2 N 0 レジスタ 5 5 および B 2 N 1 レジスタ 6 5 が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

## 【 0 0 3 9 】

なお、B 2 N 0 レジスタ 5 5 および B 2 N 1 レジスタ 6 5 を用いた演算アルゴリズムの詳細については、上述した文献を参照されたい。

## 【 0 0 4 0 】

以上説明したように、本実施の形態における暗号回路によれば、演算中に繰返し使用される固定データを予め計算して B 2 N 0 レジスタ 5 5 および B 2 N 1 レジスタ 6 5 に格納しておくようにしたので、第 1 の実施の形態において説明した効果に加えて、特定の演算に必要となるクロック数を減らすことができ、さらに演算処理を高速に行なうことが可能になった。

## 【 0 0 4 1 】

## (第 4 の実施の形態)

本発明の第 4 の実施の形態における暗号回路は、図 7 に示す第 2 の実施の形態における暗号回路と比較して、演算回路 0 ～ 3 の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

## 【 0 0 4 2 】

図 1 0 は、第 4 の実施の形態における演算回路の内部構成を説明するためのブロック図である。図 9 に示す第 3 の実施の形態における演算回路の内部構成と比較して、1 2 8 ビットの Q 0 レジスタ 7 3 および Q 1 レジスタ 7 4 が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

## 【 0 0 4 3 】

演算結果を一時的に格納しておくレジスタとして、P 0 レジスタ 7 1、P 1 レジスタ 7 2 以外に、1 2 8 ビットの Q 0 レジスタ 7 3 および Q 1 レジスタ 7 4 を設けることにより、演算結果として商と余りとをこれらのレジスタに保持することができるようになる。したがって、演算回路は、除算処理を行なうことができ

るようになる。

#### 【0044】

また、1024ビット×1024ビットの乗算を行なう場合、2048ビットの乗算結果を保持するレジスタが必要になるが、P0レジスタ71、P1レジスタ72、Q0レジスタ73およびQ1レジスタ74を用いることにより乗算結果を保持できるようになり、1024ビット×1024ビットの乗算も行なえるようになる。

#### 【0045】

以上説明したように、本実施の形態における暗号回路によれば、P0レジスタ71、P1レジスタ72以外に、128ビットのQ0レジスタ73およびQ1レジスタ74を設けることにより、第1の実施の形態において説明した効果に加えて、除算処理やビット長が長い演算データの乗算処理が行なえるようになり、逆元の生成処理や鍵の生成処理などの演算が行なえるようになった。

#### 【0046】

##### (第5の実施の形態)

本発明の第5の実施の形態における暗号回路は、図7に示す第2の実施の形態における暗号回路と比較して、演算回路0～3の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

#### 【0047】

図11は、第5の実施の形態における演算回路の内部構成を説明するためのブロック図である。図10に示す第4の実施の形態における演算回路の内部構成と比較して、128ビットのデータレジスタK0(56)およびK1(66)が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

#### 【0048】

2048ビットの演算データに対して演算を行なうには、合計2048ビットのレジスタ群を4つつ設ければよい。この場合、演算データは、4つの演算回路0～3を4周回ることになる。また、2048ビットのべき乗剰余演算を行なう場合、べきeはビット数が少なく、値が決まっており、モンゴメリ乗算剰余演



算を繰返すのに必要とされるだけである。したがって、レジスタ群を  $Y Y = \{e, Y\}$ 、 $N N = \{B 2 N, N\}$ 、 $X X = \{K, X\}$ 、 $P P = \{Q, P\}$  などのように 4 本の 2 0 4 8 ビットレジスタとして再定義し、2 0 4 8 ビットの演算アルゴリズムを実現するように制御回路を構成すれば、これに対応することができるようになる。

## 【 0 0 4 9 】

また、 $X X$  レジスタとして使用される  $K$  レジスタを他のレジスタ群と同様に利用できるように制御回路を構成すれば、加減算、乗算の実行によって中国人剰余定理による合成数を法とする演算を実現できる。さらには、加減算、乗算、除算の演算結果の符号を讀出す処理を追加することにより、拡張ユークリッド法による演算を実現できる。これによって、秘密鍵生成や中国人剰余定理に必要な逆元の計算も可能となる。

## 【 0 0 5 0 】

以上説明したように、本実施の形態における暗号回路によれば、レジスタ群を再定義してビット長が長い演算データの処理も行なえるようにしたので、第 1 の実施の形態において説明した効果に加えて、演算に必要なレジスタ数を削減でき、回路規模を縮小することが可能となった。

## 【 0 0 5 1 】

## (第 6 の実施の形態)

本発明の第 6 の実施の形態における暗号回路は、図 7 に示す第 2 の実施の形態における暗号回路と比較して、演算回路 0 ～ 3 の構成および機能が異なる点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

## 【 0 0 5 2 】

図 1 2 は、第 6 の実施の形態における演算回路の内部構成を説明するためのブロック図である。図 1 1 に示す第 5 の実施の形態における演算回路の内部構成と比較して、右シフトイン信号と左シフトイン信号とを切替える 1 ビットのセレクタ 8 1 が追加された点のみが異なる。したがって、重複する構成および機能の詳細な説明は繰返さない。

## 【 0 0 5 3 】

セレクタ 8 1 は、条件選択信号によって、右シフトイン信号を選択して出力するか、左シフトイン信号を選択して出力するかを決定する。第 1 ～ 第 5 の実施の形態においては、右シフトを実施し、左シフトを実施しない演算を行なった場合、右シフトイン信号によって入力された前段の右シフトアウトは、{Q, P} レジスタの最上位ビットに格納されると共に、左シフト回路を経由して加減算回路 3 5 に入力される。

## 【 0 0 5 4 】

このような回路構成の場合、右シフトイン信号が加減算回路 3 5 に入力されるには時間がかかるため、演算回路の動作周波数を上げることが困難になる可能性がある。本実施の形態においては、右シフトを実施し、左シフトを実施しない演算の場合には、制御回路 2 1 が条件選択信号によってセレクタ 8 1 を切替え、加減算回路 3 5 に直接右シフトイン信号を入力できるようにしている。

## 【 0 0 5 5 】

すなわち、第 1 の実施の形態においては、図 5 に示すようにクロック T 2 の立下りで P レジスタ 3 7 にデータのビット 0 ～ 1 2 6 が書込まれ、その 1 / 2 クロック後のクロック T 3 の立上りでデータのビット 1 2 7 が書込まれた。一方、本実施の形態においては、クロック T 2 の立下りで P レジスタ 3 7 にデータのビット 0 ～ 1 2 6 が書込まれ、その 1 クロック後のクロック T 3 の立下りでデータのビット 1 2 7 が書込まれる。したがって、演算回路 0 ( 4 1 ) の P レジスタ 3 7 へのビット 1 2 7 の書込み時において、上位の演算回路 1 ( 4 2 ) の右シフトアウト信号からのタイムマージンが、第 1 ～ 第 5 の実施の形態と比較して増加するし、より高い動作周波数で暗号回路を動作させることが可能となる。

## 【 0 0 5 6 】

以上説明したように、本実施の形態における暗号回路によれば、セレクタ 8 1 によって、右シフトイン信号と、{Q, P} レジスタ、左シフト回路 3 8 を経由した右シフトイン信号（左シフトイン信号）とを切替えるようにしたので、第 1 ～ 第 5 の実施の形態において説明した効果に加えて、右シフトイン信号を P レジスタ 3 7 に書込む時のタイムマージンを増加させることができ、暗号回路の動作周波数を高くすることが可能となった。

【 0 0 5 7 】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【 0 0 5 8 】

【発明の効果】

請求項 1 に記載の暗号回路によれば、第 1 の演算回路の加減算回路は、第 2 の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を第 3 の演算回路へ出力するので、演算データのデータ長が長くなってもキャリーの伝播経路を短くでき、暗号回路の動作クロック周波数を高くすることが可能となった。

【図面の簡単な説明】

【図 1】 本出願人が出願した出願書類に記載された暗号回路の概略構成を示すブロック図である。

【図 2】 演算回路 1 2 の概略構成を示すブロック図である。

【図 3】 本発明の第 1 の実施の形態における暗号回路の概略構成を示すブロック図である。

【図 4】 演算回路 0 ～ 3 （ 2 2 ～ 2 5 ） の内部構成を説明するためのブロック図である。

【図 5】 演算回路における演算データの入力タイミングおよび P レジスタ 3 7 へのデータ書込みタイミングを説明するためのタイミングチャートである。

【図 6】 演算回路における演算データの入力および P レジスタ 3 7 へのデータ書込みが連続的に行なわれる場合のタイミングを説明するためのタイミングチャートである。

【図 7】 本発明の第 2 の実施の形態における暗号回路の概略構成を示すブロック図である。

【図 8】 本発明の第 2 の実施の形態における演算回路 0 ～ 3 （ 4 1 ～ 4 4

) の内部構成を説明するためのブロック図である。

【図 9】 第 3 の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【図 1 0】 第 4 の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【図 1 1】 第 5 の実施の形態における演算回路の内部構成を説明するためのブロック図である。

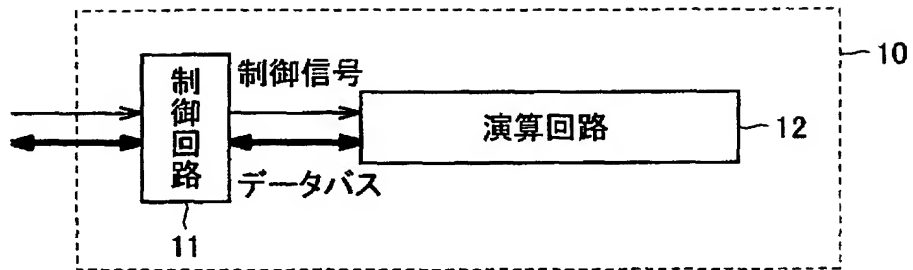
【図 1 2】 第 6 の実施の形態における演算回路の内部構成を説明するためのブロック図である。

【符号の説明】

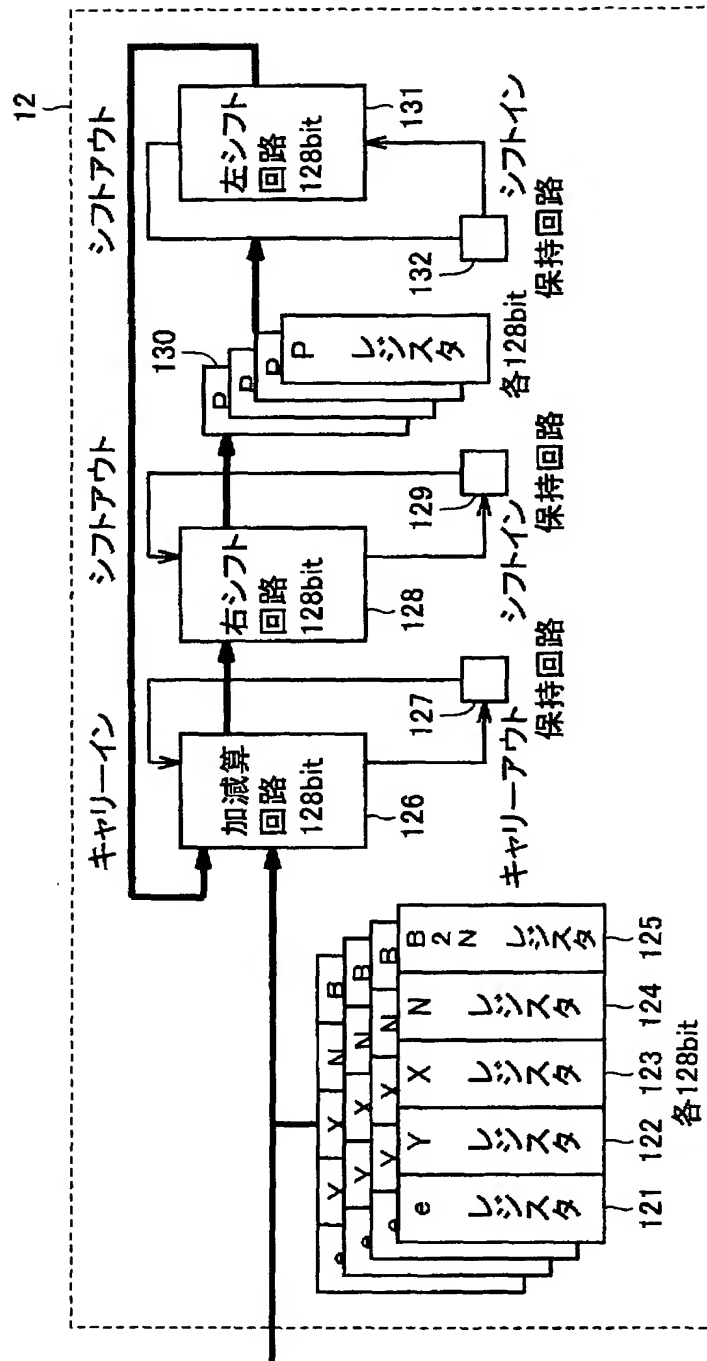
1 0, 2 0 暗号回路、1 1, 2 1 制御回路、1 2, 2 2 ~ 2 5, 4 1 ~ 4 4 演算回路、3 1, 5 1, 6 1, 1 2 1 e レジスタ、3 2, 5 2, 6 2, 1 2 2 Y レジスタ、3 3, 5 3, 6 3, 1 2 3 X レジスタ、3 4, 5 4, 6 4, 1 2 4 N レジスタ、3 5, 1 2 6 加減算回路、3 6, 1 2 8 右シフト回路、3 7, 7 1, 7 2, 1 3 0 P レジスタ、3 8, 1 3 1 左シフト回路、5 5, 6 5, 1 2 5 B 2 N レジスタ、5 6, 6 6 K レジスタ、7 3, 7 4 Q レジスタ、8 1 セレクタ、1 2 7, 1 2 9, 1 3 2 保持回路。

【書類名】 図面

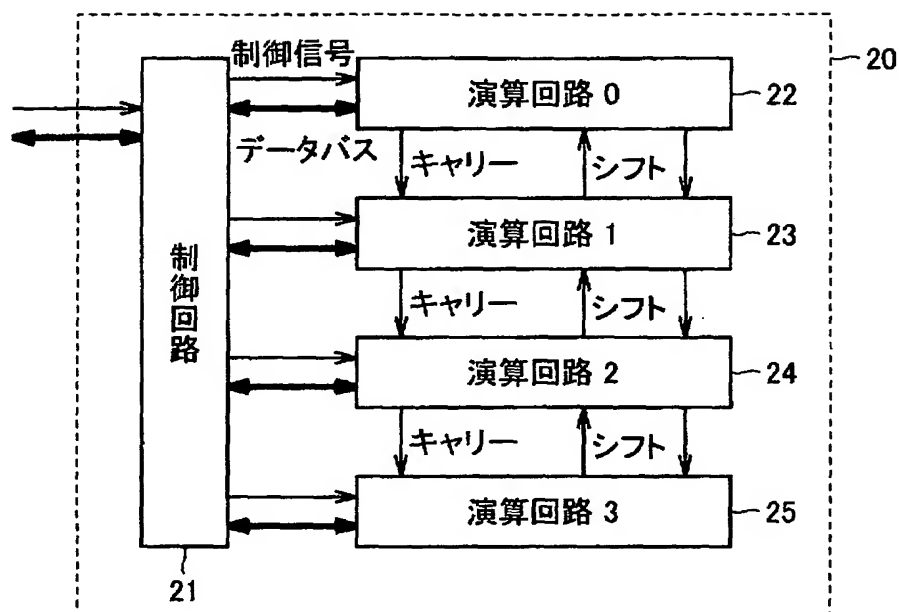
【図 1】



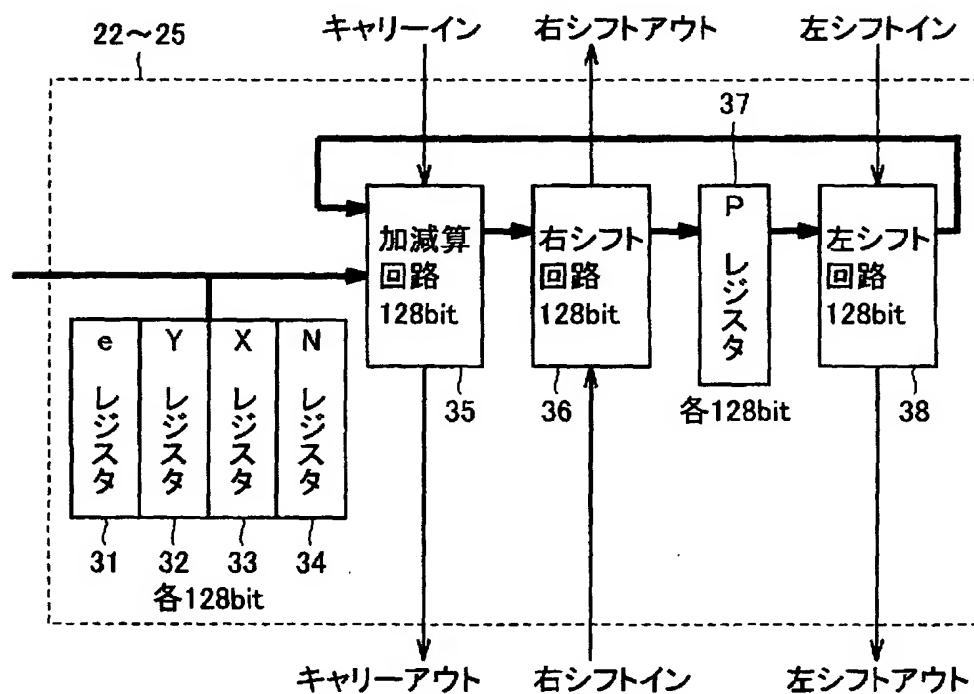
【図 2】



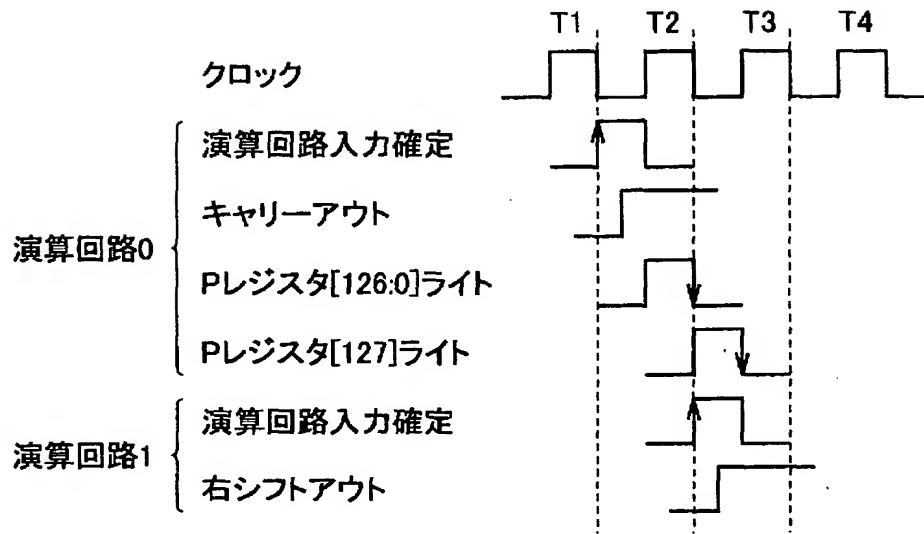
【図 3】



【図 4】

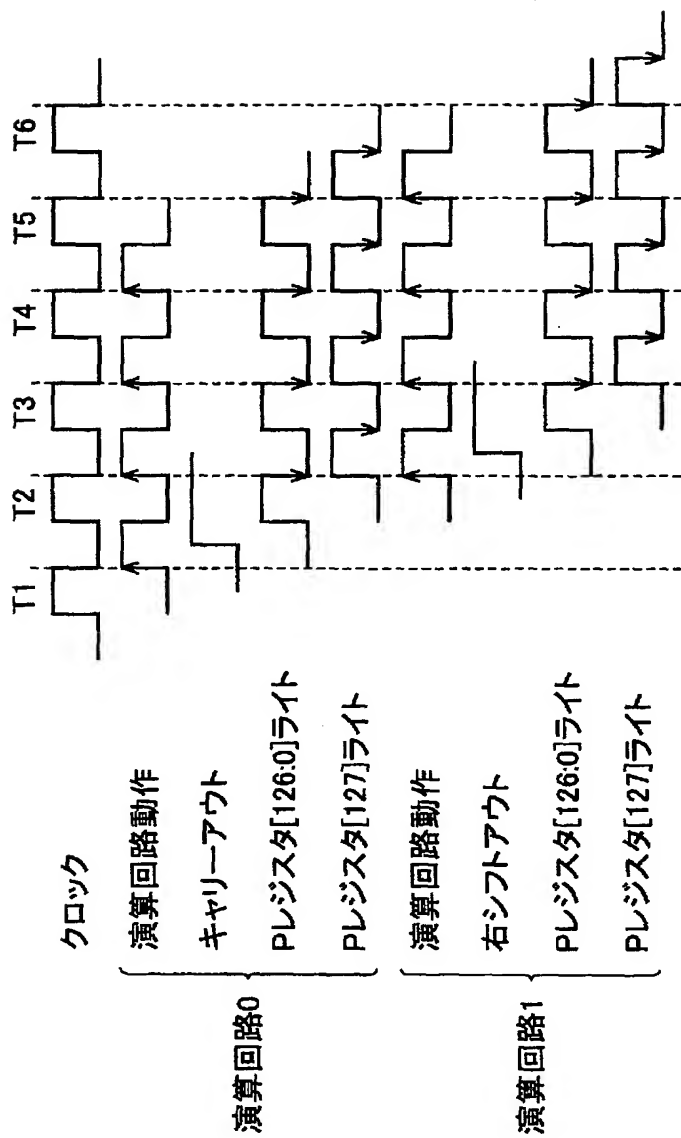


【図 5】

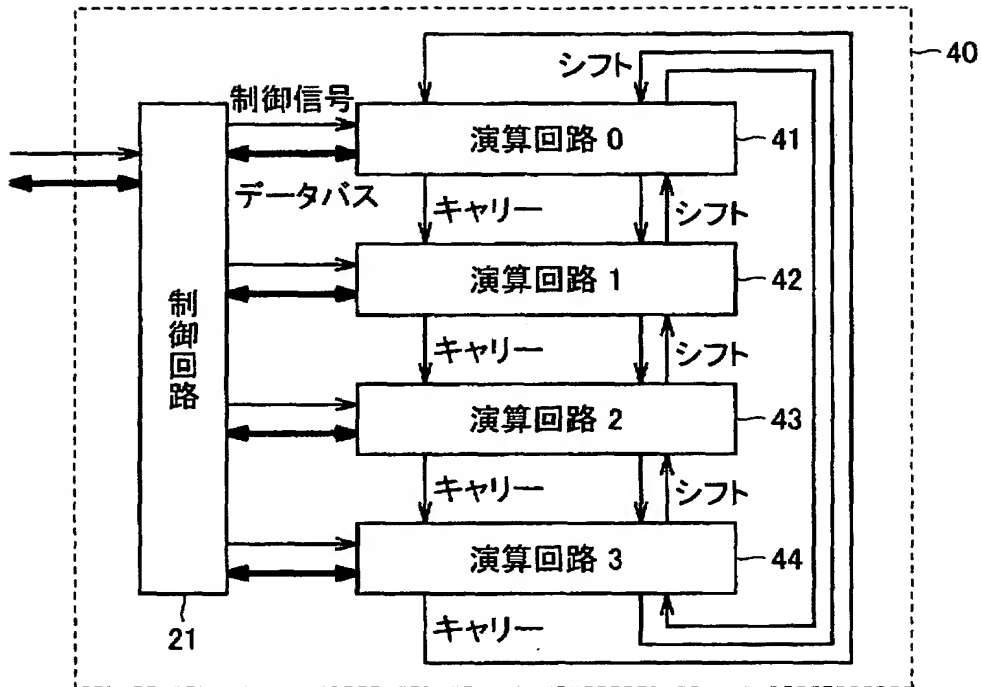




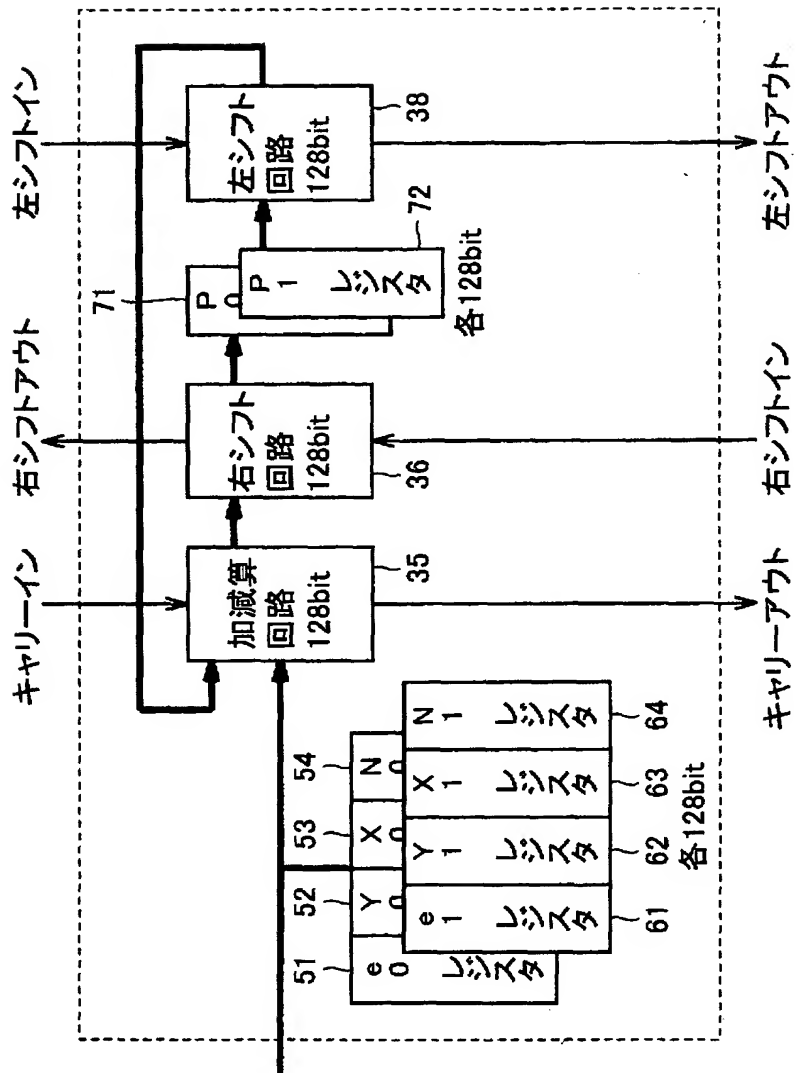
【図6】



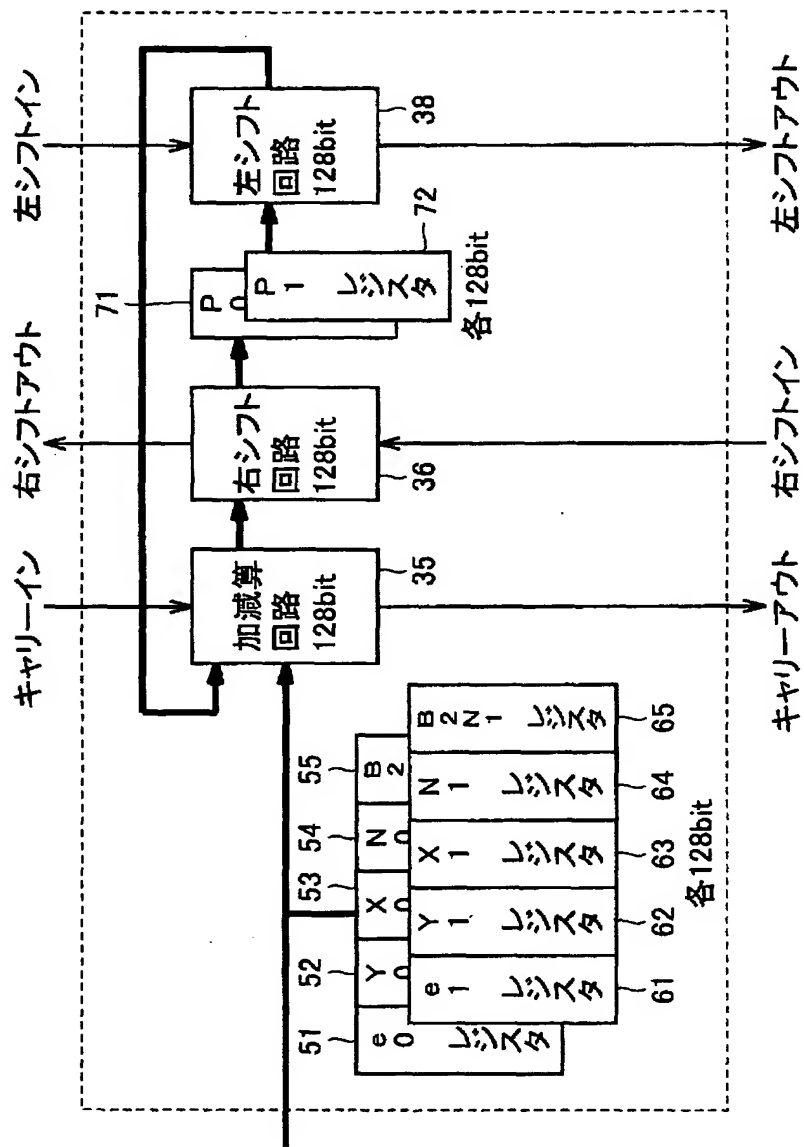
【図 7】



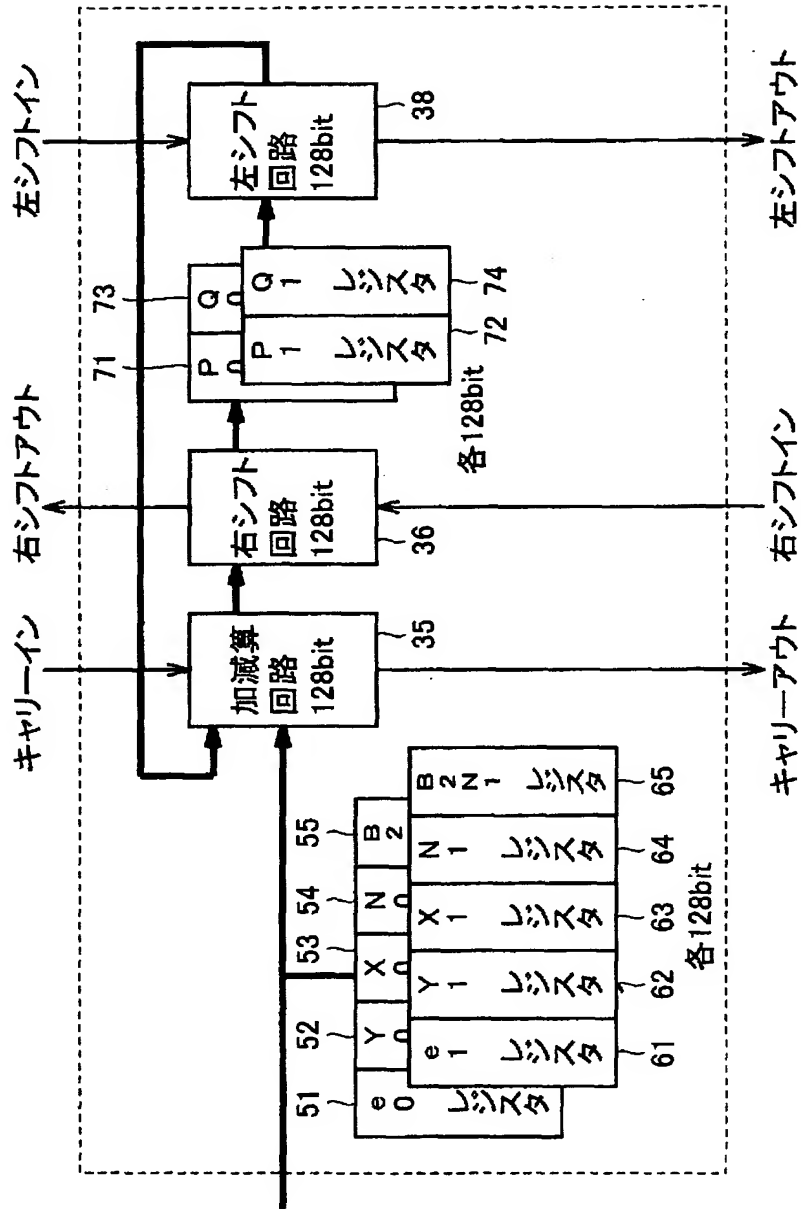
【図 8】



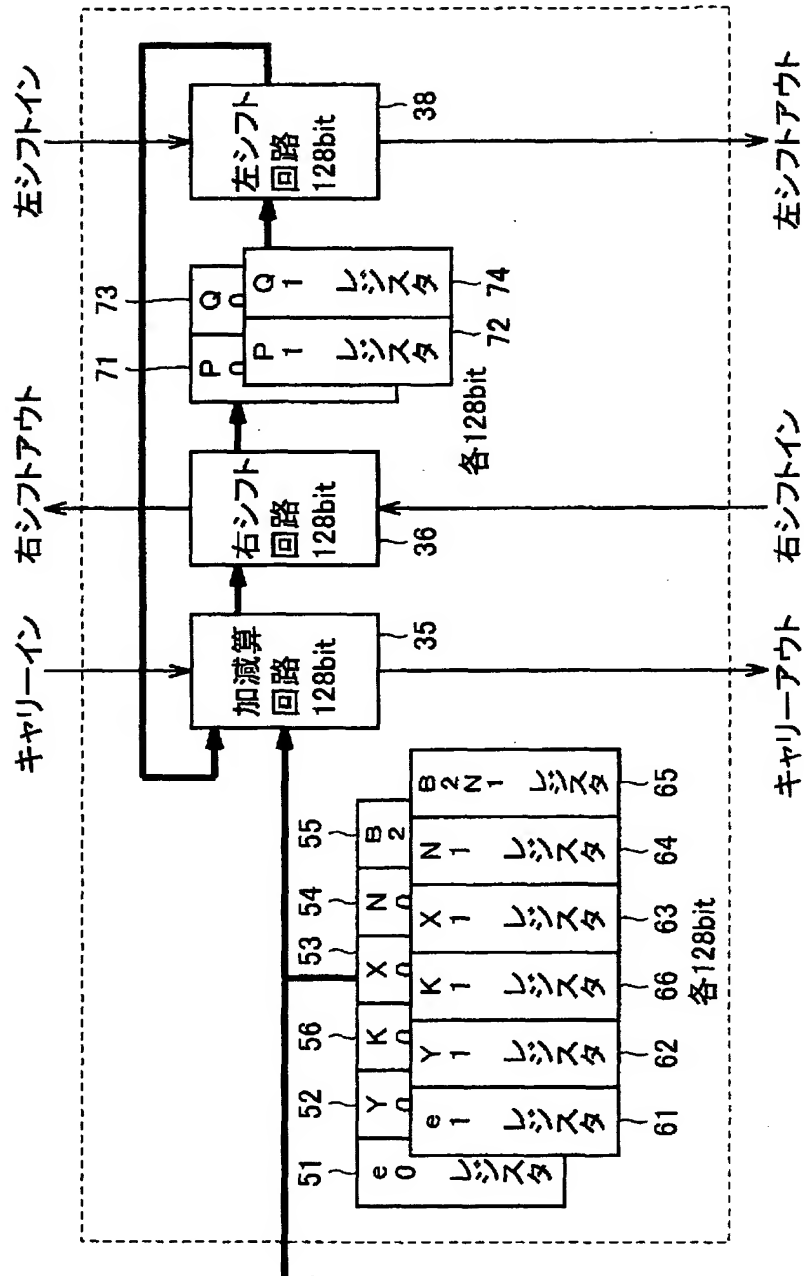
【図9】



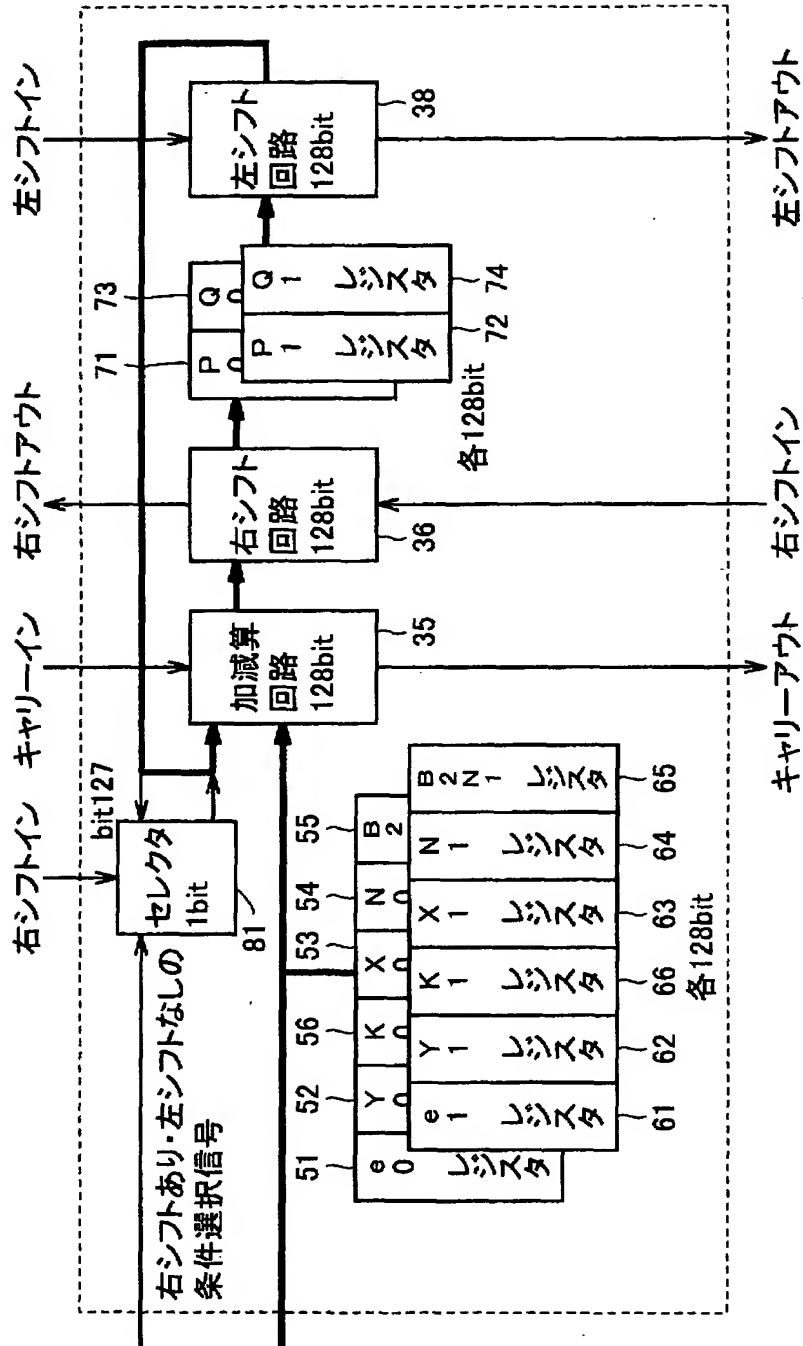
【図10】



【図 11】



【図12】



【書類名】            要約書

【要約】

【課題】    暗号回路の動作クロック周波数を高くでき、演算速度の高速化を図ることが可能な暗号回路を提供すること。

【解決手段】    加減算回路 3 5 は、他の演算回路からのキャリーイン信号を用いて加減算を実行し、加減算によって発生したキャリーアウト信号を他の演算回路へ出力する。また、右シフト回路 3 6 は、他の演算回路からのシフトイン信号を用いて右シフトを実行し、右シフトによって発生するシフトアウト信号を他の演算回路へ出力する。したがって、演算データのデータ長が長くなってもキャリーの伝播経路を短くでき、暗号回路の動作クロック周波数を高くすることが可能となる。

【選択図】            図 4



出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社